UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,909	04/06/2006	Vincent Carlier	4005-0277PUS1	7126

2292 7590 06/14/2007

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
06/14/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/574,909	CARLIER ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/6/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1- 5 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 06 April 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Application Publication No. 2004/0187035 to Schwan et al., hereinafter Schwan.

6. As per claim 1, Schwan teaches a method of protecting a cryptographic algorithm (paragraphs 0007, 0013, i.e. destroying or erasing a cryptographic algorithm so an unauthorized person does not obtain knowledge of the algorithm) for execution in a device comprising programmable processor unit (paragraph 0010, microprocessor and programmable memory), wherein the algorithm is DES (paragraph 0015) and implemented on the programmable processing unit (paragraph 0002).

7. On page 5, lines 22-30 of the Specification, the Applicant admits that the DES algorithm is known, and wherein it is necessary for DES to combine more than two initial polynomials in order to obtain combined polynomials. Therefore, Schwan discloses the steps of combining polynomials from at least two initial polynomials and implementing the combined polynomials in the programmable processor unit.

8. Regarding claim 2, Schwan teaches the step of storing the encryption algorithms in the form of a configuration file that is loaded into a memory associated with the processor unit (paragraph 0002, i.e. updating the control program, programming the control unit to a customer and application needs, modify the functional and performance range of the control unit, reprogramming the control unit).

9. With regards to claim 3, Schwan teaches wherein the memory and the programmable processor unit are associated with an eraser member serving, in the event of an intrusion into the device, to erase the processor unit, and to erase the memory containing the configuration file when the configuration is present in said memory (paragraph 0013, i.e. encryption algorithm is erased and/or destroyed after the housing is opened (the intrusion)).

10. Regarding claim 4, Schwan discloses the use of DES (paragraph 0013). As noted above DES combines more than two initial polynomials in order to obtain combined polynomials. DES also includes a function f_k and f_k^{-1}. This is supported by the disclosure of DES in **Cryptography and Network Security, Principles and Practices**, by William Stallings, hereinafter Stallings.

Specifically, Stallings discloses the function f_k on at least page 61, or the initial permutation as disclosed on page 57. Stallings goes on further to discuss on page 57 the inverse initial permutation towards the end of the cryptographic calculation. Therefore Schwan teaches the step of combining each combined polynomial (Q_k) with a function (f_k), and of combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}) in his disclosure of DES.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schwan in view of **Applied Cryptography, Protocols, Algorithms, and Source Code in C**, by Bruce Schneier, hereinafter Schneier.

13. With regards to claim 5, Schwan does not teach wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the initial permutation, or claimed function f_k, be a linear function, since Schneier states at page 271 that the initial permutation is used to transpose the input block of data, and as such a linear function would make it easier to transpose the input block and load the plaintext and ciphertext into a DES chip in byte-sized pieces.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

16. The following patents are cited to further show the state of the art with respect to erasing cryptographic algorithms, such as:

United States Patent No. 6,556,681 to King, which is cited to show a universal transmitter that destroys cryptographic material when the system has been compromised.

United States Patent No. 7,191,219 to Udell et al., which is cited to show destroying documents and e-mails after a certain period or when the data has been compromised.

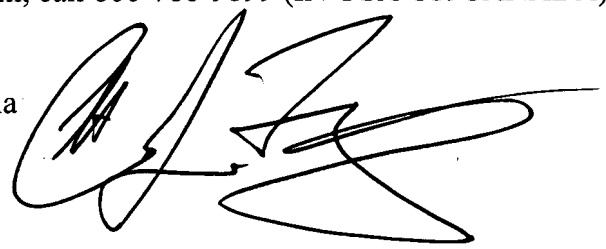
United States Patent Application Publication No. 2005/0005147 to Fischer et al., which is cited to show protecting cryptographic calculations in a cryptographic algorithm.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf